REMARKS

Claims 1-8, 28-29, 31-34 are pending in this application. By this Response, claims 1, 3, 28, and 33 are amended. Claim 1 is amended to correct a typographical error and to clarify the phrase "each of" by repositioning it in the claim as requested by the Examiner. Claim 3 is amended for clarification purposes only. Claims 28 and 33 are amended to remove the phrase "adapted to provide" as suggested by the Office Action. Claim 33 is further amended to delete the last two lines which were deemed unclear by the Office Action. No new matter has been introduced by any of the above amendments. Furthermore, all of the above amendments are made only for clarification purposes and do not raise any new issues requiring further search or consideration. Thus, entry of the above amendments after the mailing of the Final Office Action is proper. Accordingly, Applicants respectfully request entry of the above amendments and reconsideration of the claims in view of the above amendments and the following remarks.

I. Telephone Interview

Applicants thank Examiner Gergiso for the courtesies extended to Applicants' representative during the February 5, 2010 telephone interview. During the telephone interview, the above amendments and the distinctions of the claims over the cited art were discussed. Examiner Gergiso agreed to enter the above amendments, which are only of a clarifying nature, and further consider the claims as explained by Applicants' representative during the telephone interview.

As discussed at length during the telephone interview, the underlying difference between the presently claimed invention and the cited prior art is that the presently claimed invention determines whether a next device (whether that next device is an intermediate device or the final target device) along a path provides a required level of security as specified in a header of the object that is being transmitted and then transmitting the object to the next device only if it provides the required level of security. The cited references verify that the source of data that is being transmitted is a valid source (Suzuki) and establish a least common denominator policy among all the nodes of

a path prior to performing any transmission of data (Lee). Thus, if the cited art were combined, it would result in a mechanism in which the least common denominator policy is established before transmission and then as the data is being transmitted from one device to another, a check is made as to whether the source of the data is a valid source or not. The alleged combination of references would not result in the invention as claimed in the present application.

The substance of the telephone interview is summarized in the following remarks.

II. Allowable Subject Matter

Applicants thank Examiner Gergiso for the indication of allowable subject matter in claims 3 and 5. However, for the reasons set forth hereafter, Applicants respectfully submit that all of the claims are directed to allowable subject matter and that the application is in condition for allowance.

III. Claim Objections

The Office Action objects to claims 1, 28, and 33 for various informalities. By this Response, claims 1, 28, and 33 are amended where appropriate to eliminate these formalities. Accordingly, Applicants respectfully request withdrawal of the objection to claims 1, 28, and 33.

IV. Rejection under 35 U.S.C. § 112, Second Paragraph

The Office Action rejects claims 1, 3, and 5 under 35 U.S.C. § 112, second paragraph as being allegedly indefinite. This rejection is respectfully traversed.

With regard to claim 1, the Office Action alleges that because the claim recites at least three devices, i.e. a source device, an intermediate device, and a target device to form the path that somehow this invalidates the recitation of "a next device in the transmission path" and renders the claim indefinite. Applicants respectfully disagree.

Simply reciting at least 3 devices does not invalidate a recitation of a "next device." If one is transmitting from a first device to a second device, then the second device is the "next device" along the path. Thus, for example, if the transmission is going from the source device to the intermediate device, then the intermediate device is the "next device" along the path. Similarly, if the intermediate device is transmitting to a target device, then the target device is the "next device" along the path. The phrase "next device" along the path is specifically used in the claims because there may actually be more than one intermediate device and thus, it is possible that the "next device" is not a single intermediate device or the target device, but can be a second, third, fourth, etc., intermediate device. All that is required is that a determination is made as to whether a "next device" in the transmission path, be that any one of the one or more intermediate devices or the target device, to which the object is to be transmitted, provides a level of security indicated by at least a portion of the security information in the header of the object. Thus, the recitation of the phrase "a next device in the transmission path" does not render the claim indefinite.

Regarding claim 3, it is Applicants' understanding that the Office Action alleges that the claim does not recite a plurality of alternatives from which "at least one of" the alternatives is performed. By this Response, claim 3 is amended to more clearly recite the alternatives by replacing the term "and" with "or." Accordingly, Applicants respectfully submit that claim 3 clearly recites the alternatives of either "transmitting information representative of the level of security that is desired to the next device in the transmission path which prompts the next device in the transmission path to execute at least one module that allows the next device in the transmission path to provide the level of security *or* comparing the next device in the transmission path to a list of trusted devices in the header portion of the object.

In view of the above, Applicants respectfully request withdrawal of the rejection of claims 1, 3, and 5 under 35 U.S.C. § 112, second paragraph.

V. Rejection under 35 U.S.C. § 103(a)

The Office Action rejects claims 1-2, 4, 6-8, 28-29, and 31-34 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Suzuki (U.S. Patent Application Publication No. 2004/0259529) in view of Lee (U.S. Patent Application Publication No. 2005/0188072). This rejection is respectfully traversed.

Independent claim 1 reads as follows:

> 1. A method, comprising:
>
> determining security information associated with an object of a transaction, wherein the security information is inserted in a header of the object and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;
>
> ***determining, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header of the object***; and
>
> transmitting, at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, the object to the next device in the transmission path ***in response to determining that the next device provides the level of security required by the at least a portion of the security information***.
>
> (emphasis added)

Applicants respectfully submit that neither Suzuki nor Lee, either alone or in combination, teach or render obvious at least the features of claim 1 emphasized above.

Suzuki is directed to a wireless adhoc communication system in which frame transmission source authentication is performed among terminals involved in delivery of the frames. Specifically, a first terminal generates a keyed hash value by using an authentication header key determined with respect to a second terminal and gives it to an authentication header of a frame. The second terminal generates a keyed hashed value by using the authentication header key determined with respect to the first terminal and compares it with the authentication header given to the frame. If the keyed hashed value

generated at the second terminal matches the authentication header ***it is confirmed that the frame has been transmitted from the first authenticated valid terminal***. The first terminal encrypts a payload part by using a unicast encryption key determined with respect to a third terminal. This encrypted payload part can be decrypted only by the third terminal having the unicast encryption key (see Abstract of Suzuki).

Thus, essentially Suzuki is directed to validating that a frame is being sent from an authenticated valid terminal. Suzuki is not concerned with determining whether a next device along a transmission path provides a level of security indicated by at least a portion of the security information in the header of an object being transmitted. To the contrary, Suzuki is specifically looking backward to the source to determine if the source was valid. At no time in the operation of the wireless adhoc communication system of Suzuki is there any determination as to whether the next target of the transmission provides a required level of security as specified in a header of the frame.

Moreover, nowhere in Suzuki is there any teaching or technical rationale provided for transmitting an object along the transmission path to the next device in response to determining that the next device provides a level of security required by the portion of the security information in the header of the object. To the contrary, in Suzuki, the frame is transmitted only when it is determined that the *source* of the frame, i.e. the terminal that is attempting to transmit, is an authenticated valid terminal. Suzuki is not concerned with whether the next device to which the frame is being transmitted provides a required level of security as specified in a header of the frame.

The Office Action points to paragraphs [0011], [0021], [0044], [0050], and [0073]-[0074] of Suzuki as teaching these features (Office Action, pages 4-5). These paragraphs of Suzuki read as follows:

> [0011] In one form of the terminal of the present invention, the terminal may further include: a path table having at least one path list for holding a transfer destination terminal identifier for causing a frame to arrive at another terminal in such a manner as to correspond to the terminal identifier of the other terminal; and means for searching the path table for the path list containing an end-point terminal identifier and transmitting the frame to the transfer destination terminal identifier when the authentication header is valid and the end-point terminal identifier of the frame is not the terminal identifier of the other terminal and for discarding

the frame when the authentication header is not valid. As a result, an operational effect is obtained such that, ***when the fact that the authentication header given to the received frame is generated by a valid transmission terminal is confirmed, the frame is transferred to the next transfer destination terminal, and if the authentication header is not valid, the frame is discarded.***

[0021] In another aspect, the present invention provides an encryption method for use in a terminal having a key management list table having at least one key management list for holding authentication header keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of the other terminals, the encryption method including the steps of: searching the key management list table for the key management list containing the reception terminal identifier of a frame to be transmitted in order to extract the corresponding authentication header key; generating a keyed hashed value, in which the extracted authentication header key is hashed together with a predetermined area of the frame, and giving the keyed hashed value as an authentication header to the frame; and transmitting the frame. As a result, an operational effect is obtained such that the reception terminal is made to confirm that a valid authentication header is given on the basis of the keyed hash function, whose strength is ensured.

[0044] The terminal B receiving the frame confirms whether or not the authentication header 809 is valid by using the authentication header key (AHK_AB) with respect to the terminal A. When it is confirmed that the authentication header 809 is valid, the terminal B generates an authentication header 809 by using an authentication header key (AHK_BC) with respect to the terminal C which is the next transmission source and gives the authentication header to the frame. In that case, the encrypted payload part 802 is transmitted as is. On the other hand, if the authentication header 809 is not valid, the frame is discarded without being delivered to the next transmission source.

[0050] The authentication header 809 is authentication data used to perform frame transmission source authentication. An authentication header key (AHK) is determined in advance between the transmission terminal and the reception terminal. Then, in the transmission terminal, a keyed hashed value, in which a predetermined area of a transmission frame and the authentication header key are hashed together, is generated, and this hashed value is given as the authentication header 809. In the reception terminal, a keyed hashed value, in which a predetermined area of a reception frame and the authentication header key are hashed together, is generated, and this hashed value is compared with the authentication header 809. If the result of this comparison shows a match,

it is confirmed that the received frame has been transmitted from the transmission frame.

[0073] Furthermore, the terminal A generates the authentication header key (AHK_AB) (133). The authentication header key is generated randomly or on the basis of a random number in the manner described above. This authentication header key should be changed as appropriate. The terminal A encrypts the generated authentication header key (AHK_AB) in accordance with the public key (PK_B) of the terminal B, and transmits it as an authentication header key distribution message 1342 to the terminal B (134). The terminal B receiving the authentication header key distribution message 1342 decrypts the authentication header key in accordance with the secret key of the terminal B itself (234).

[0074] The terminal A and the terminal B set the authentication header key (AHK_AB) obtained in this manner in the key management list table 670 (FIG. 6) of its own terminal (135, 235). That is, the terminal A sets the authentication header key (AHK_AB) in the column of the authentication header key 673 of the key management list having the terminal B as the terminal identifier 671. The terminal B sets the authentication header key (AHK_AB) in the column of the authentication header key 673 of the key management list having the terminal A as the terminal identifier 671. In this manner, the terminals which form the wireless adhoc communication system share the authentication header key with respect to the adjacent terminal.

Paragraph [0011] merely teaches a path list and that the frame is only transmitted when the source of the frame is authenticated; otherwise it is discarded. The citation of paragraph [0011] only serves to bolster Applicants' position that Suzuki teaches authenticating the source of a frame, not determining whether a next device along the path provides a required security level as specified in a header of an object that is to be transmitted.

Paragraph [0021] merely teaches a key management table for terminals and using the keys in the key management table to get the key for the terminal to which the frame is to be transmitted and hashing a piece of the frame with the key and then transmitting the frame. While this paragraph mentions getting a key for a terminal to which the frame is being transmitted, this paragraph does not make any mention of determining whether a next device along a transmission path provides a level of security indicated by at least a portion of the security information in the header of the frame. To the contrary, the

encryption using the key is merely a way of authenticating that the frame came from an authorized valid terminal.

Paragraph [0044] merely teaches an example in which terminal B confirms that the authentication header of a frame is value using an authentication header key with respect to terminal A (from which the frame was sent). If it is confirmed, then terminal B generates an authentication header for terminal C and transmits the frame with the new authentication header to terminal C. Again, this is merely to authenticate that the frame is being sent from an authorized valid terminal, i.e. the header generated by terminal B would be invalid if terminal B did not already know the key for terminal C.

Paragraph [0050] merely teaches that the key is determined ahead of time between the source and the target of the transmission and that this key is used by the target to generate an encrypted portion of a frame that can then be compared against the encryption value in the header to determine if the frame is coming from an authenticated valid terminal. Again, this is merely teaching a mechanism for authenticating the source of a frame, not determining whether a next device along a transmission path provides a required level of security as specified by security information in a header of an object being transmitted.

Paragraphs [0073]-[0074] merely describes a flowchart outlining the operation discussed above with regard to using a key to generate a hashed value that can be compared against a value in a header of a frame to determine if the frame is coming from an authenticated valid source. Thus, it is clear from the above that the cited portions of the Suzuki reference, in actuality, do not teach or render obvious the specific features of claim 1 as emphasized above.

The Office Action admits that Suzuki does not teach security information that is associated with a transaction object or providing a level of security indicated by at least a portion of the security information (see Office Action, page 5). However, the Office Action alleges that these features are taught by Lee. Applicants respectfully disagree.

Lee is directed to a mechanism for dynamically constructing a protocol to facilitate communication between nodes and across multiple nodes. Policies associated with the nodes are used to specify protocol properties of the nodes. A policy expression in a policy related to a node can be selected by another node to construct a protocol

between the two nodes. A policy expression selection process can be applied to multiple nodes in a communication path to construct a protocol across the multiple nodes (see paragraph [0007]). A computer can retrieve an intermediate node policy characterizing communication properties supported by the intermediate node and may request destination node policies characterizing communication properties supported by a destination node (paragraphs [0009]-[0010]).

With Lee, the protocol must be established first before any actual message communications are performed between a source and a destination. Lee provides a mechanism for establishing such a protocol dynamically based on the policies of the nodes between the source and destination. Essentially, the mechanism of Lee creates a protocol that is supported by all of the nodes along a communication path prior to performing any communication. This essentially means that the protocol that is created has a minimum number of protocol properties according to the lowest common denominator amongst the nodes.

Lee does not provide any teaching, or technical rationale, to implement the features of providing security information in a header of an object of a transaction, at least a portion of the security information identifying a required level of security required for each device along a transmission pathway, or using the portion of the security information at each device along the transmission pathway to determine if a next device along the pathway provides the required level of security and transmitting the object to the next device if the next device provides the required level of security. To the contrary, Lee is concerned with connection level protocol establishment, rather than providing a transaction level security mechanism, as is recited in claim 1. Lee is not concerned with performing security level checks on each individual device of a transmission path, whether the individual device provides a level of security required by header information an object of a transaction prior to the object being transmitted to the device and transmitting the object to that device in response to a determination that the device supports the required level of security.

In summary, the Suzuki reference uses keys and hash values to authenticate that data is being transmitted from a valid *source*. Suzuki does not teach checking the next device to which the data is to be transmitted to see if the next device provides a required

level of security as specified in the header of the data to be transmitted. Thus, Suzuki essentially looks backwards to see if the data is coming from a valid source whereas the claimed invention looks forward to see if the next device provides the required level of security before transmitting the data. Thus, Suzuki does not teach or render obvious the features of the claimed invention. Moreover, the Lee reference also does not teach or render obvious these features as discussed above. Hence, any alleged combination of Suzuki and Lee, even if such a combination were possible and one were somehow motivated to attempt such a combination, *arguendo*, would still not result in the features of independent claim 1 being taught or rendered obvious.

These distinctions, likewise, apply to similar features in independent claim 28. That is, independent claim 28 specifically recites determining if the first device ***provides a level of security identified by the at least a portion of security information in the header of the object***; transmitting an indication to the second device, based on determining if the first device provides the level of security identified by the at least a portion of security information; and receiving, in the first device, the object from the second device ***only in response to the first device transmitting an indication that the first device provides the level of security identified by the at least a portion of security information***. As noted above, neither Suzuki nor Lee, either alone or in combination, teach or render obvious such features.

In view of the above, Applicants respectfully submit that the alleged combination of Suzuki and Lee fails to teach or render obvious at least those features of independent claim 1 or the similar features in independent claim 28. At least by virtue of their dependency on claims 1 and 28, respectively, Suzuki and Lee fail to teach or render obvious the features of dependent claims 2, 4, 6-8, 29, and 31-34. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-2, 4, 6-8, 28-29, and 31-34 under 35 U.S.C. § 103(a).

In addition, dependent claims 2-8, 29, and 31-33 recite additional features that are not taught or rendered obvious by the alleged combination of Suzuki and Lee. For example, with regard to claim 2, the alleged combination of references fails to teach transmitting to the next device in the transmission path information representative of the level of security that is desired or receiving a response from the next device in the

transmission path indicating that the next device in the transmission path provides the desired level of security. The Office Action alleges that these features are taught by Lee at paragraphs [0011], [0034], and [0037] which read as follows:

> [0011] In yet another implementation, a system includes a source node policy having protocol parameters related to a source node and a policy retriever retrieving an intermediate node policy having protocol parameters related to and intermediate node between the source node and a destination node in a communication path. The system also includes a message generator generating a request message in accordance with the intermediate node policy, the request message including a request for a destination node policy having protocol parameters related to the destination node.
>
> [0034] The policy retriever 134 retrieves policies from other nodes, such as node B 104 or intermediate nodes on the network 106. The policy retriever 134 can request a policy from another node, receive the policy, and may cache a received policy in memory for later use. The policy retriever 134 can also retrieve a policy that was previously stored in local memory on node A 102. The policy retriever 134 also performs functions related to determining whether a retrieved policy is compatible with a local policy and/or selecting a compatible policy expression in a retrieved policy.
>
> [0037] The policy retriever 140 at node B 104 has functionality similar to the functionality described above with respect to policy retriever 134 at node A 102. The message generator 142 at node B 104 formats and transmits messages to node A 102 in accordance with one or more assertions in the input policy 108 of node A 102.

Paragraph [0011] merely teaches that the system includes a source node policy, a policy retriever for retrieving an intermediate node policy, and a message generator that generates a request message. Paragraph [0034] merely teaches that the policy retriever retrieves policies from other nodes by requesting the policy from another node, receiving the policy, and caching the received policy or retrieving the policy from local memory. The retriever can also determine if the retrieved policy is compatible with a local policy and select a compatible policy expression in the retrieved policy. Paragraph [0037] merely teaches that node B's policy retriever operates in the same way as the policy

retriever of node A and has a message generator that transmits a message in accordance with an input policy of node A.

While these sections of Lee talk about policy retrieval for intermediate nodes, nothing in these sections, or any other sections, of Lee mention or render obvious the specific features of transmitting to the next device in the transmission path information representative of the level of security that is desired or receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security. To the contrary, Lee retrieves the policy for the intermediate node and determines compatible expressions in the intermediate node's policy that are compatible with the policy of the source node. Lee does not transmit information to the intermediate node information representative of a level of security that is desired. Moreover, Lee does not receive a response indicating that the next device in the transmission path provides the desired level of security.

As a further example, regarding claim 6, the alleged combination of Suzuki and Lee fails to teach or render obvious the features of determining an alternative device along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next device in the transmission path does not provide the level of security required by the at least a portion of the security information. The Office Action alleges that these features are taught by Lee at paragraphs [0083]-[0088] and [0100].

Paragraphs [0083]-[0088] read as follows:

> [0083] The operations described above pertain to environments in which one node is communicating with another node using dynamic protocol construction. Often, in actual operation, messages from one node are routed through other nodes before reaching the destination node. For example, in a corporate environment, messages may be routed through a firewall, a main server, and finally to a recipient's computer. Each node in the path may have policies related to data protocols that are preferred, available, and/or required by the node.
>
> [0084] FIG. 5 illustrates an exemplary multiple node communication environment 500 including a source node 502 and a destination node 504. A message exchange occurs between the source node 502 and the destination node 504, via two intermediate nodes, intermediate node X

506, and intermediate node Y 508. Source node 502, destination node 504, intermediate node X 506, and intermediate node Y 508 each have a policy. The policy at each node can include one or more policies (e.g., input policy, output policy), as discussed above. ***In general, the source node 502 retrieves policies in order from closest node to farthest node, and applies policies to a message in order from farthest node to closest node, as is illustrated by an exemplary scenario below.***

[0085] Source node 502 generates a message intended for the destination node 504. As discussed above, source node 502 retrieves the policy of the destination node 504, in order to select a policy expression, and apply the selected policy expression to the message. However, in order to retrieve the policy of the destination node 504, the source node 502 must go through intermediate node X 506 and intermediate node Y 508.

[0086] In the exemplary scenario described with respect to the environment 500, it is assumed that source node 502 initially has no information about (i.e., is not aware of) the presence of intermediate node Y 508, but is aware of intermediate node X 506. ***In order to retrieve the policy from destination node 504, the source node 502 first requests the policy from intermediate node 506. The source node 502 selects a policy expression from the policy related to intermediate node X 506 and applies the selected policy expression to a policy retrieval message.***

[0087] The policy retrieval message is a request for the policy from the destination node 504. Included with the policy retrieval message is the policy related to the source node 502. The intermediate node X 506 receives the policy retrieval message, including the policy of the source node 502, and validates the message, as discussed above, by checking to see that a valid policy expression was applied to the policy retrieval message. If the policy retrieval message is valid, the intermediate node X 506 requests the policy from the destination node 504.

[0088] ***The intermediate node X 506 puts the policy of the destination node 504 into a message for the source node 502. This includes applying the policy of the source node 502 to the message so that the message to the source node 502 conforms to the policy of the source node 502. The source node 502 receives and validates the message and reads the policy of the destination node 504.***

Paragraphs [0083]-[0088] describe a process of getting the destination node policy by obtaining policy from an intermediate node, selecting a policy expression from the policy of the intermediate node and applying it to a policy retrieval message that includes the policy for the source node. The intermediate node receives the policy retrieval message,

validates it based on the valid selected policy expression that was applied to the policy retrieval message, and then requests the policy from the destination node. The intermediate node then places the policy of the destination node into a message for the source node by applying a policy of the source node to the message and sending it back to the source node. Thus, the policies are used to authenticate the source of policy information.

Nothing in these sections teaches or renders obvious the specific features of determining an alternative device along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next device in the transmission path does not provide the level of security required by the at least a portion of the security information. There is not even the mention of an alternative device anywhere in any of these paragraphs. Thus, contrary to the allegations raised in the Office Action, these sections of Lee do not in fact teach or render obvious the specific features of claim 6.

With regard to paragraph [0100], Lee is stating that the mechanism of Lee determines if a node requires routing to another node, i.e. a routing assertion. This does not teach anything about determining an alternative device along a different transmission path ***that provides the level of security required*** by the at least a portion of the security information ***if the next device does not support the level of security required***. All that Lee is stating here is that if a node specifies another node to which it must route communications, Lee identifies that.

Regarding claim 7 (and claim 29), the alleged combination of references fails to teach or render obvious the specific feature of sending a message to the next device in the transmission path instructing the next device to execute at least one module that allows the next device to provide the level of security required by the at least a portion of the security information. The Office Action again points to paragraphs [0083]-[0088] of Lee as allegedly teaching this feature. However, as shown above, these paragraphs only describe retrieving a destination policy by retrieving an intermediate node policy, selecting a compatible expression from the policy to authenticate a request for the destination policy, sending the request to the intermediate node which authenticates the request based on the compatible expression and requests the policy from the destination

node. The intermediate node then sends a message back to the source using a compatible expression selected from the source policy, the message including the destination node policy. Nowhere in this process is there any mention of sending a message to a next device instructing that device to execute a module that allows the next device to provide a level of security required by the at least a portion of the security information, as recited in claim 7.

With regard to claim 31, this claim recites a specific implementation of the method of claim 1 in which there are two intermediate nodes and where in the method is first implemented at the source node with regard to the first intermediate node being the "next node" in the transmission path and then the performing the method at the first intermediate node (which then operates as the "source node") with regard to a second intermediate node (which then operates as the "next node" in the transmission path). Just as with claim 1 above, the alleged combination of Suzuki and Lee fails to teach or render obvious the features of claim 31. The Office Action points to many different sections of Lee as allegedly teaching the specific features of claim 31 but none of these paragraphs or Figures actually teach any of these features. In fact, it is unclear what the Examiner's position is since many of these features, which are specific applications of the methodology of claim 1 to specific nodes, i.e. source, first intermediate, second intermediate, and target nodes, which were alleged to be taught by Suzuki are now instead alleged as being taught by Lee. Which is it? Does Suzuki teach these features or does Lee teach these features? It is unclear what the Examiner believes is equivalent to these features since the Examiner takes two different positions with regard to the same references. Regardless, for similar reasons as set forth above, Applicants respectfully submit that neither Suzuki nor Lee, either alone or in combination, teach or render obvious the specific features of claim 31.

Regarding claim 32, this claim recites similar features to claim 6 discussed above. However, instead of citing paragraphs [0083]-[0088] and [0100] as in the rejection of claim 6, the Examiner instead cites paragraphs [0054] and [0100] in the rejection of claim 32. Paragraph [0100] has been addressed above with regard to the rejection of claim 6. Paragraph [0054] of Lee merely teaches that a policy allows a node to specify capabilities, requirements, the number of messages and their form, security measures,

reliable messaging, transactions, routing, and other parameters relevant to a message exchange. This does not provide any relevant teaching to the particular features of claim 32. Stating that a policy allows a node to specify capabilities, requirements, etc. does not teach or render obvious the feature of determining an alternative intermediate device along a different transmission path that provides a level of security represented in response to determined that at least one of the first intermediate device and the second intermediate device in the transmission path does not provide the level of security. wherein the at least one intermediate device includes a plurality of intermediate devices;

With regard to claim 33, the alleged combination of Suzuki and Lee fails to teach or render obvious the features of determining if a next device in the transmission path provides a level of security comprises determining, at a previous device in the transmission path, a security level for each intermediate device of the plurality of intermediate devices. Moreover, the alleged combination fails to teach or render obvious the features of transmitting the object to the next device in the transmission path, in response to determining that the next device provides the level of security, comprises transmitting the object to each of the plurality of intermediate devices in the transmission path in response to determining that each of the plurality of intermediate devices provides the level of security.

The Office Action points to paragraphs [0084], [0094], and [0100] of Lee as allegedly teaching all of these features. Paragraph [0100] is reproduced above. Paragraphs [0084] and [0094] read as follows:

> [0084] FIG. 5 illustrates an exemplary multiple node communication environment 500 including a source node 502 and a destination node 504. A message exchange occurs between the source node 502 and the destination node 504, via two intermediate nodes, intermediate node X 506, and intermediate node Y 508. Source node 502, destination node 504, intermediate node X 506, and intermediate node Y 508 each have a policy. The policy at each node can include one or more policies (e.g., input policy, output policy), as discussed above. ***In general, the source node 502 retrieves policies in order from closest node to farthest node, and applies policies to a message in order from farthest node to closest node, as is illustrated by an exemplary scenario below.***

> [0094] Thus, the policy-compliant message 512 that is sent from the source node 502, may be viewed as a message with three levels of policy application. ***The policy-compliant message 512 includes an inner level of policy application 514 that relates to the destination node 504 and will be received and validated last in the message exchange. The policy-compliant message 512 includes a middle level of policy application 516 related to the intermediate node Y 508 and will be received and validated next-to-last in order. The policy-compliant message 512 includes an outer level of policy application 518 related to the intermediate node X 508 and will be received and validated first in the message exchange.***

While these paragraphs teach that the message includes multiple layers of policies that are retrieved from the nodes along a path to a destination node, there still is no teaching in any of these sections regarding determining, at a previous device in the transmission path, ***a security level for each intermediate device of the plurality of intermediate devices***. Moreover, there is no teaching of transmitting the object to each of the plurality of intermediate devices in the transmission path ***in response to determining that each of the plurality of intermediate devices provides the level of security***. All that Lee teaches is that the policies of the nodes are gathered and applied to a message in a layered manner. This does not teach or render obvious the specific features of claim 33.

Regarding claim 34, the alleged combination fails to teach or render obvious the features of the object being one of a plurality of objects of the transaction, and wherein at least two of the objects in the plurality of objects have different security information in their respective headers identifying different levels of security required to be provided by devices along corresponding transmission paths to receive the at least two objects. The Office Action again points to paragraphs [0083]-[0088] and [0100] of Lee as allegedly teaching these features. These paragraphs are addressed and reproduced above. It is plainly evident from the above that there is not even the mention of objects, let alone multiple objects of a transaction or at least two objects of the same transaction having different levels of security required by devices along the transmission path. There simply is no correlation between what is described in the cited paragraphs and the features of claim 34.

Thus, in view of the above, Applicants respectfully submit that dependent claims 2-8, 29, and 31-33 are further distinguished over Suzuki and Lee by virtue of the specific features recited in these claims.

VI. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: February 9, 2010

Stephen J. Walder

Stephen J. Walder, Jr.
Reg. No. 41,534
Walder Intellectual Property Law, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPLICANTS